Enoncé TP – avec int64

Etant donné qu'en RUST, il n'est pas évident de gérer les nombres codés sur plus de 128 bits (nécessaires dans ce cas), le problème a été re-codé avec des clés plus petites. Expliquez pourquoi, dans ce cas, le message codé comprend plus de blocs !

$$n = 2901984751$$
$$e = 9103$$

-----Message codé -----
1780565330
1418927598
543482106
729172139
111350267
2866131698
353182206
2750311025
1740400630
2336243297
570711647
2642624210
1208279921
2741398971
381511738
1701929578
2875813324
1677894499
1797737510
2901354249
1627727243
762227604
756639409
600478187
2152502192
10636100
2133402040
1181530544
46461495
1681846270
432128454
-----Fin message Codé-----

Vous travaillez en tant qu'espion pour une agence gouvernementale et devez à tout prix décoder le message envoyé à vos ennemis.

Tout ce dont vous disposez sont des informations publiques et du message codé via l'algorithme RSA.

La clé publique est la suivante :

$$n = 19395215754271188593$$
$$e = 471131$$

Votre intuition vous dit que les deux premiers utilisés pour générer la clé publique ont le même ordre de grandeur et que le message utilise l'encodage UTF-8 standard (8 bits par charactère).

Le message intercepté est composé de divers paquets comme suit :

----- Message Codé -----
1213428545899287006
128066609881241950
1524544144808352117
5739320063815598366
5318541268334496831
10099198048166427552
1294578297747087516
5219535363202696744
8873085490801871488
9767440483961474498
6090604250892558071
7230451814471929172
16327068223369301731
3332316276070559024
-----Fin Message Codé -----

Faites un rapport décrivant comment vous avez déchiffré le message.

Faites également une analyse de la performance de votre approche, et estimez le temps qu'il vous faudrait pour déchiffrer une clé ayant non pas 20 chiffres, mais 200 !!!